ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

March 20, 2000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

Honorable John W. Warner
Chairman,
Committee on Armed Services
United States Senate
Washington, DC 20510-6050

Dear Mr. Chairman:

Enclosed is the Department of Defense report to the congressional defense committees as requested on page 196 of Report 106-244 on the Department of Defense Appropriations Bill, 2000, July 20, 1999. The report describes lessons learned from the Year 2000 effort and their applicability to information assurance.

We appreciate this opportunity to share with you the significant changes in information technology management resulting from the Year 2000 effort.

Sincerely,

Arthur L. Money

Enclosures:
As Stated

cc:
Honorable Carl Levin
Ranking Minority

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

March 20, 2000

Honorable Ted Stevens
Chairman, Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510-6028

Dear Mr. Chairman:

Enclosed is the Department of Defense report to the congressional defense committees as requested on page 196 of Report 106-244 on the Department of Defense Appropriations Bill, 2000, July 20, 1999. The report describes lessons learned from the Year 2000 effort and their applicability to information assurance.

We appreciate this opportunity to share with you the significant changes in information technology management resulting from the Year 2000 effort.

Sincerely,

Arthur L. Money

Enclosures:
As Stated

cc:
Honorable Daniel K. Inouye
Ranking Minority

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

March 20, 2000

Honorable Jerry Lewis
Chairman, Subcommittee on Defense
Committee on Appropriations
United States House of Representatives
Washington, DC 20515-6018

Dear Mr. Chairman:

Enclosed is the Department of Defense report to the congressional defense committees as requested on page 196 of Report 106-244 on the Department of Defense Appropriations Bill, 2000, July 20, 1999. The report describes lessons learned from the Year 2000 effort and their applicability to information assurance.

We appreciate this opportunity to share with you the significant changes in information technology management resulting from the Year 2000 effort.

Sincerely,

Arthur L. Money

Enclosures:
As Stated

cc:
Honorable John P. Murtha
Ranking Minority

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

March 20, 2000

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

Honorable Floyd Spence
Chairman,
Committee on Armed Services
United States House of Representatives
Washington, DC 20515-6035

Dear Mr. Chairman:

Enclosed is the Department of Defense report to the congressional defense committees as requested on page 196 of Report 106-244 on the Department of Defense Appropriations Bill, 2000, July 20, 1999. The report describes lessons learned from the Year 2000 effort and their applicability to information assurance.

We appreciate this opportunity to share with you the significant changes in information technology management resulting from the Year 2000 effort.

Sincerely,

Arthur L. Money

Enclosures:
As Stated

cc:
Honorable Ike Skelton
Ranking Minority

Report to

Congressional Defense Committees

As Requested In

Report of the Committee on Appropriations on the

Department of Defense Appropriations Bill, 2000

Report 106-244

YEAR 2000 (Y2K) Lessons Learned

March 15, 2000

Table of Contents

Introduction

The Department of Defense (DoD) treated the Year 2000 (Y2K) as a cyber attack directed at the very core of its military capabilities - the ability to obtain, process and control information that allows American forces to dominate the battlefield. The DoD military and civilian leadership dealt with Y2K as a readiness issue and attacked the problem accordingly.

Securing DoD information systems for Y2K afforded numerous lessons that will translate well in efforts to secure critical information infrastructures in the future. Our efforts led to the best ever accounting of DoD systems and their status. An information management structure now in place meets the requirements of the Clinger-Cohen Act. Senior leaders are more aware and appreciate information technology, including the need for government to keep pace with industry. In many ways, we can look back on Y2K as a blessing that forced America to face realities of a rapidly changing information-based world.

Thanks to the tireless efforts of people throughout DoD, there were no major problems on January 1, 2000. Over the 18 months leading up to the century rollover, however, several important things happened. Getting ready for the Year 2000 (Y2K) had many positive impacts throughout the Department of Defense (DoD), including:

- Improved integrated working relationships between DoD Chief Information Officers, warfighters, and senior leaders
- Thousands of people worked to make systems compliant and ensure Y2K readiness
- The Commanders-in-Chief (CINCs) of the unified commands, the military departments, and the defense agencies and activities have a much better understanding of their information technology systems and interdependencies
- DoD shifted from a system focus on information technology to a core mission and function approach
- DoD greatly reduced Y2K risk through a series of risk mitigation measures including: 123 major end-to-end evaluations, screening of computer software code using automated tools, and special configuration management policies and procedures
- DoD greatly upgraded and improved contingency plans for individual system failure and for ensuring continuity of operation
- DoD established on-going discussions for greater assurance on host nation support
- DoD better understands the dependencies on critical infrastructures outside its control that are necessary to accomplish core missions

DoD Y2K Program

Scope, Magnitude and Complexity

The scope and complexity of the Y2K problem for the DoD is unparalleled in the federal government. The DoD has over 3 million people – active, Guard, Reserve, and civilian – spread all over the world. To administer this community takes over 1.5 million individual computers at hundreds of locations around the globe. For the Y2K problem, the DoD tracked 9,634 systems, of which 25 percent (2,367) were considered mission critical systems. The Department also operates 637 military installations around the world and in the United States, which are like small towns, and rely on supporting infrastructure systems also vulnerable to Y2K problems. In addition, the Department had 15 centralized mainframe computer sites comprising 351 computer domains in operation on January 1, 2000. Over one-third of the government's mission critical systems are in the DoD.

Senior Leadership Involvement

The DoD made enormous efforts to ensure Y2K readiness. In August 1998, Secretary Cohen directed DoD's leadership to treat the Y2K issue as a major threat to military readiness. The Chairman of the Joint Chiefs of Staff was directed to include Y2K testing in joint warfighting and operational readiness exercises. The Military Departments and Defense Agencies were instructed to fix their systems, certify interfaces, and ensure vendors were held responsible for Y2K compliance of products. Finally, officials on the Secretary's staff were told to ensure functioning of specific business processes, such as medical and health activities, finances and payments, personnel, logistics, communications, and intelligence.

Major Phases of DoD Y2K Program

The DoD Y2K program evolved throughout the Y2K preparation period. In all, the program had three major components: Achieving Systems Y2K Compliance, Large Scale Integration Testing, and Risk Reduction Efforts.

Achieve Y2K System Compliance

The three major parts of achieving system compliance were: the five phase Office of Management and Budget management process; reliance on centralized guidance with decentralized execution; and a centralized inventory of information technology systems.

Five Phase OMB Management Process

The DoD adopted the Office of Management and Budget five-phase management process and institutionalized it in the DoD Y2K Management Plan. Extensive auditing throughout the DoD helped ensure that compliance with the five-phase system compliance process was relatively uniform and reported results were accurate.

Centralized Guidance, Decentralized Execution

The DoD established the DoD Y2K Management Plan as the central vehicle for conveying guidance on Y2K preparations throughout the department. The use of one document, available on-line, helped ensure all parts of DoD were working towards the same goal using the same approved procedures and tools.

Establish a Centralized Inventory of Information Technology Systems

To ensure a uniform baseline of systems and to implement common performance measurement standards to gauge progress, DoD established a centralized inventory of information technology systems. This DoD Y2K database was an essential management tool combining user level input with data quality assurance measures and managerial reviews. By using an on-line methodology, the DoD was able to continually shorten the reporting cycle as the Y2K program evolved to ensure an accurate and timely representation of DoD Y2K readiness.

Large Scale Integration Testing

The DoD executed a complex and multi-faceted approach to evaluation focused on improving confidence in the Department's ability to execute the National Military Strategy. The DoD concentrated on complex, real-world end-to-end testing of "business functions" and Warfighter missions necessary to carrying out the national military strategy.

The DoD evaluation efforts were extremely complex and many events occurred nearly simultaneously. The Services conducted integration testing of functional or mission threads. The functional staff proponent on the Office of the Secretary of Defense (OSD) staff organized and conducted end-to-end evaluations of core functional capabilities. Finally, the Commanders in Chief (CINCs) of combatant commands selected unique missions to devise real-world operational evaluations assessing the ability to execute warfighting tasks in a Y2K environment.

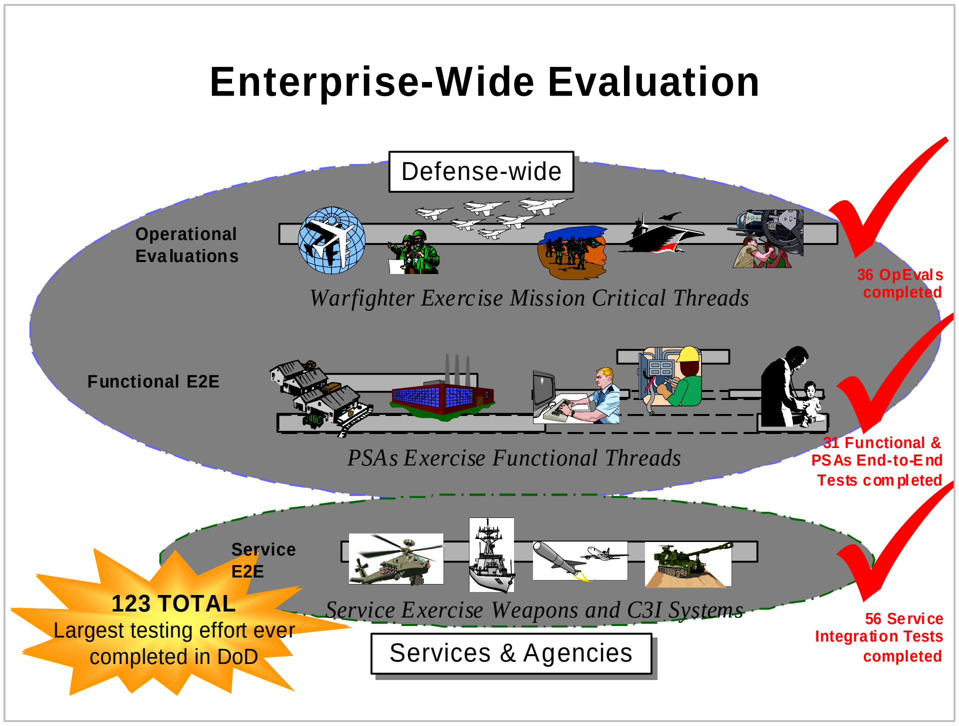
The number of activities, finite amount of resources (particularly testing experts and time), and demands of real world day-to-day operations forced an iterative and highly centralized synchronization of the entire evaluation plan. Evaluation efforts were managed in sessions co-chaired by members of the OSD staff and the Joint Staff. The DoD Inspector General provided oversight and another review to search for holes in the evaluation program. Finally, the General Accounting Office also provided external audit.

The key events in the DoD evaluation plan were CINC Operational Evaluations, functional end-to-end evaluations, and Military Department end-to-end and integration testing. The DoD conducted 36 operational evaluations, 31 major end-to-end tests, and 56 large-scale system integration tests, a total of 123 major Y2K evaluations. These evaluations involved thousands of people and systems worldwide, including Navy Battle Groups, Army Divisions, Air Force Wings, Marine Expeditionary Units, and Defense Agencies and Activities.

CINC Operational Evaluations

The DoD assessed operational readiness by validating the warfighting process, from "sensor-to-headquarters" using the significant dates specified by the General Accounting Office Testing Guide. Results confirmed that this kind of evaluation was essential to providing the additional assurance that systems would remain operational over the Y2K transition.

The CINCs of the combatant commands conducted 36 operational evaluations of a representative sample of warfighting systems. Because live fire evaluation of weapons systems was not feasible during CINC operational evaluations, critical weapons and other warfighting systems were evaluated by the military departments during integration testing.



Enterprise-Wide Evaluation

Defense-wide

Operational Evaluations

Warfighter Exercise Mission Critical Threads

36 OpEvals completed

Functional E2E

PSAs Exercise Functional Threads

31 Functional & PSAs End-to-End Tests completed

Service E2E

Service Exercise Weapons and C3I Systems

56 Service Integration Tests completed

Services & Agencies

123 TOTAL
Largest testing effort ever completed in DoD

Functional End-to-End Testing

The principal staff assistants of the OSD staff coordinated end-to-end tests of business function processes such as logistics, medical, personnel, communications, intelligence and finance. The Department used its business process managers to evaluate the capability to continue core support functions despite Y2K.

In some functional areas, particularly logistics, the Military Departments conducted end-to-end evaluations of their internal functional systems before DoD-wide functional evaluations. These tests were in addition to the CINC operational evaluations and included, in many cases, organizations and systems outside of DoD.

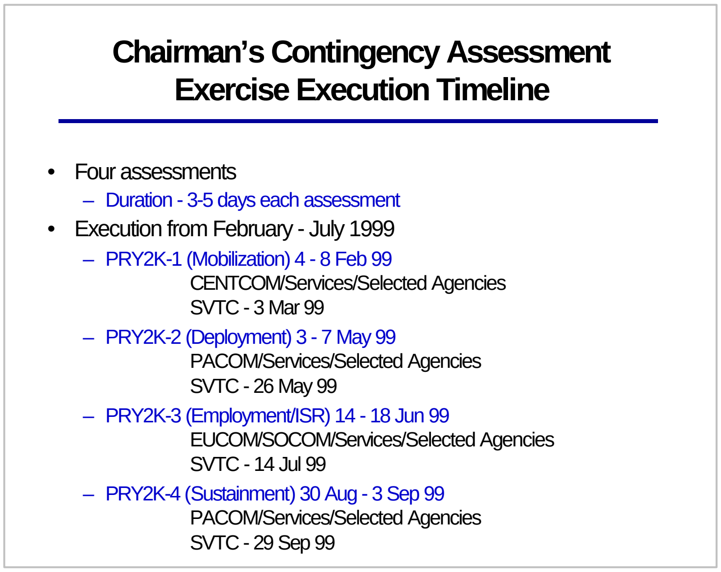
Military Department End-to-End Testing

Integration testing by the Military Departments ensured continued functioning of key processes such as organizing, training, and equipping forces. This testing was over and above the five-phase Office of Management and Budget process each individual system completed to achieve certification as Y2K compliant.

The Military Department integration testing was a critical factor in ensuring the ability of Service Components to carry out their parts of the CINC warfighting plans and provided a useful foundation prior to more complex, real-world CINC operational evaluations. The successful testing of several weapons systems (Kiowa, Apache, Hellfire, and Multiple Launch Rocket System) at White Sands, New Mexico, for example, provided an excellent basis for future CINC operational evaluations.

Chairman of the Joint Chiefs of Staff (CJCS) Contingency Assessments

The CJCS conducted Exercise POSITIVE RESPONSE Year 2000 (PRY2K), a series of four command post exercises scheduled from February to September 1999. These were the first national level exercises conducted under conditions of multiple Y2K mission critical system failures. The PRY2K assessed the ability of DoD to respond with timely decisions in a Y2K degraded environment and focused on the strategic national tasks of mobilization, deployment, employment, intelligence-surveillance-reconnaissance, and sustainment. This series of exercises was designed to achieve senior participation in and awareness of the operational impact of Y2K mission critical systems failure during mobilization, deployment, employment, and sustainment processes. The concept was to remove mission critical systems and capabilities from play during the conduct of a robust warfighting scenario and then assess DoD ability to respond with timely decisions. In addition, the exercises assessed the ability of the Services to execute operational contingency plans and to mitigate problems associated with Y2K. Finally, senior members of the warfighting community shared lessons learned and other vital information via secure videoteleconference. The Secretary of Defense, CJCS, Service Chiefs, and CINCs participated in the videoteleconference following each exercise with a goal of recommending a strategy to the National Command Authorities to mitigate the impact of mission critical systems failure.



Chairman's Contingency Assessment
Exercise Execution Timeline

- Four assessments
  - Duration - 3-5 days each assessment
- Execution from February - July 1999
  - PRY2K-1 (Mobilization) 4 - 8 Feb 99
    CENTCOM/Services/Selected Agencies
    SVTC - 3 Mar 99
  - PRY2K-2 (Deployment) 3 - 7 May 99
    PACOM/Services/Selected Agencies
    SVTC - 26 May 99
  - PRY2K-3 (Employment/ISR) 14 - 18 Jun 99
    EUCOM/SOCOM/Services/Selected Agencies
    SVTC - 14 Jul 99
  - PRY2K-4 (Sustainment) 30 Aug - 3 Sep 99
    PACOM/Services/Selected Agencies
    SVTC - 29 Sep 99

Business Continuity and Contingency Planning (BCCP)

As with other aspects of the Y2K effort, the DoD approach to BCCP was to provide centralized policy guidance with DoD components developing plans based on that guidance and executing them appropriately. While some planning assumptions changed for individual plans, the overall DoD BCCP guidance remained valid. A brief summary of BCCP follows.

Business Impact Analysis

Impact analysis was performed using operational risk analysis procedures standard for all DoD planning processes. Extremely long and complex information chains characterize most DoD missions. To ensure that these chains were thoroughly examined, the Joint Staff, each of the CINCs, the Services, and most DoD Agencies used a technique called *Thin Line of Systems*

Analysis. This technique determined critical paths by which information flowed during the execution of primary missions. Identifying the *thin lines* served to ensure that all mission-critical systems were identified for each DoD mission/function. Systems comprising these *thin lines* were all involved in end-to-end testing to ensure that all elements were fully Y2K compliant.

Core Functions

The Department of Defense is a very complex organization. Under its present organization, there are three primary allocations of responsibility. These are:

> **Warfighting**, which is the responsibility of the Joint Chiefs and the Unified Commands;
>
> **Organize, Train and Equip**, which are the Title 10 responsibilities of the Military Departments; and
>
> **Support Functions** (Logistics, Personnel, Health/Medical, Communications, Intelligence, and Finance) which are the responsibilities of designated Principal Staff Assistants on the OSD staff.

The DoD commands receive missions from various higher authorities. These missions can be analyzed and linked to elements from the applicable Service or Joint Mission Essential Task List (METL). The missions and METL of each DoD command correspond to the core functions of that command.

Planning Assumptions

There are two major categories of planning assumptions: general assumptions applicable across DoD, and site specific assumptions applicable to a unique location.

General Planning Assumptions

Operations in DoD occur worldwide and thus the general planning assumptions were separated into Continental United States (CONUS) and outside CONUS (OCONUS) locations.

CONUS

To prepare BCCP, DoD components assumed that electric power, natural gas, water service, waste treatment, financial services, transportation, the Internet, public voice and data communications, mail service, and the mass media would be available domestically with possible localized disruptions. Each command prepared operational contingency plans determining the degree to which the general assumption applied to their sites(s).

OCONUS

In non-U.S. locations, DoD followed the general planning assumptions of the State Department, which, in cooperation with other agencies, gathered Y2K information on a country-specific basis. The State Department designated the Head of Mission in each country as the U.S. lead on Y2K issues there. Agencies with interests overseas worked with the State Department to understand the risks to their operations and to develop appropriate assumptions.

Site-Specific Planning Assumptions

The commander or director responsible for each DoD site or facility was responsible for determining the appropriate site-specific planning assumptions for that location. This entailed due diligence in seeking out the Y2K status of local suppliers of critical services and supplies to that site in support of its core functions.

Other Risks to DoD Operations

The principal external risks to DoD operations were separated into three categories: Domestic Infrastructure Disruptions, Host Nation Infrastructure Support Disruptions, U.S. and North Atlantic Treaty Organization (NATO)/Allied Systems Interoperability Disruptions.

Domestic Infrastructure Disruptions

Domestic infrastructure disruptions were addressed during the normal contingency planning process. DoD planners made full use of the extensive information available through the Internet and the large number of DoD Y2K-related web sites.

Host Nation Infrastructure Support Disruptions

Regional discussions with host nations for OCONUS installations were used to ensure that Y2K planning assumptions are valid, as discussed previously. In addition, the DoD Y2K Office had representatives working directly with NATO to facilitate the process of information exchange among NATO planners. Since the most critical status updates were those in the final months before the century rollover, this process grew in emphasis during 1999.

NATO/Allied Systems Interoperability Disruptions

Interoperability testing was planned and conducted to ensure systems interoperability with Allied and NATO systems. The operational contingency plans developed by Joint and Allied Commands addressed procedures to be followed in case of unforeseen disruptions.

In summary, DoD BCCP efforts were designed to ensure the continued ability to operate regardless of Y2K-related disruptions. As shown during the century rollover, for the isolated instances when system problems occurred, the contingency plan was successfully executed to ensure continued operations with minimal disruption.

Risk Reduction

The three major components of DoD’s risk reduction efforts were leadership preparations, global outreach, and a group of risk mitigation policies.

Leadership Preparations

Table Top Exercises

In addition to the CJCS Contingency Assessments, DoD announced its plan for preparing senior leadership for the impact of Y2K on national security in a December 8, 1998, memorandum titled, “Participation in Department of Defense and National Level Y2K Table Top

Exercises." This memorandum outlined exercise activities conducted at the defense and national level. The exercises exposed participants to a reasonably worst case scenario induced by potential Y2K failures. These activities enhanced participants' understanding of potential Y2K impacts on national security; assisted in developing policy recommendations; provided continuing impetus to accelerate progress on fixing Y2K systems problems; and facilitated effective contingency planning. The four-part program is in the figure below.

- A set of three functionally oriented one-day policy seminars held in November and December 1998 that identified some 70-80 policy-level issues that formed the foundation for further Table Top Exercise activities.
- A daylong Table Top Exercise policy workshop held on January 30, 1999. Participants represented the key decision-makers of DoD, including the Deputy Secretary of Defense, the State Department, the Federal Emergency Management Agency (FEMA), the President's Y2K Coordinator, and congressional staffers.
- A DoD Defense/National Security game conducted on September 8, 1999, and completed before the national level exercise. The DoD game focused on policy and crisis management in response to a national security emergency. The DoD senior leadership fully participated, including the Deputy Secretary of Defense, the Vice-Chairman of the Joint Chiefs of Staff, the Service Under Secretaries, the DoD Chief Information Officer, selected Principal Staff Assistants and the Directors of specified Defense Agencies. The State Department and FEMA also participated in the exercise.
- This activity led to a National-level Y2K Table Top Exercise on September 18, 1999. This White House inter-agency exercise was supported jointly by DoD and FEMA.

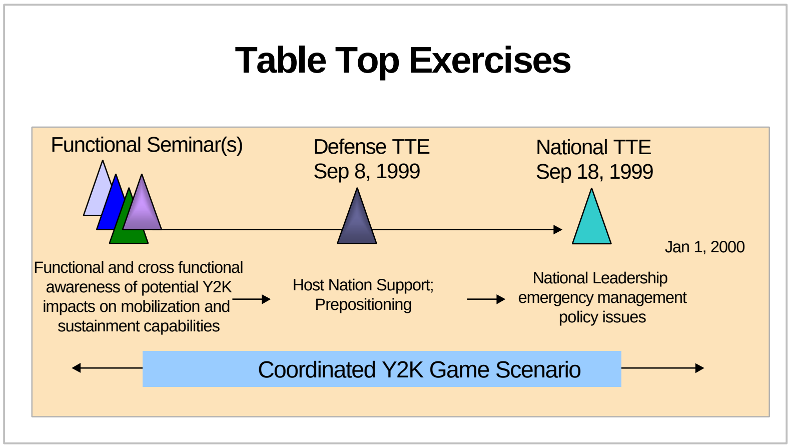


Table Top Exercises
Functional Seminar(s)
Defense TTE
Sep 8, 1999
National TTE
Sep 18, 1999
Jan 1, 2000
Functional and cross functional awareness of potential Y2K impacts on mobilization and sustainment capabilities
Host Nation Support; Prepositioning
National Leadership emergency management policy issues
Coordinated Y2K Game Scenario

Secretary of Defense Y2K Posture Message

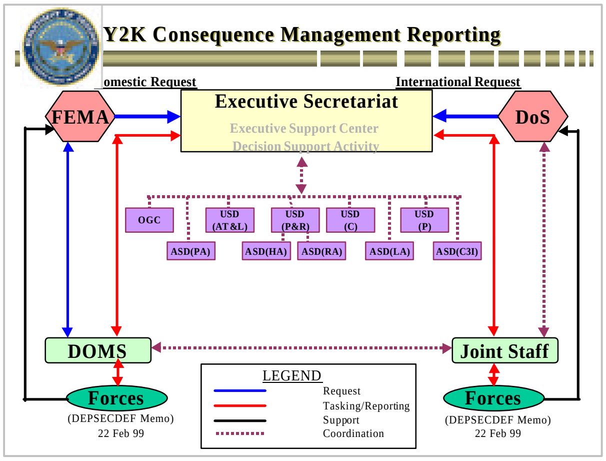
To ensure uniform preparedness for the Y2K rollover period, the Secretary of Defense issued a Y2K Posture message that specified the level of readiness required for all DoD components in preparing for Y2K rollover events. These posture levels provided planning and action assumptions for DoD components and a means to synchronize actions in anticipation of or response to any disruptions occurring during the date transition.

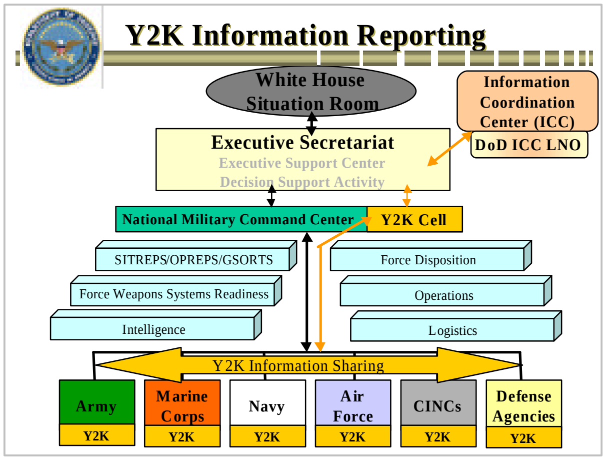
Reporting and Tracking Y2K Rollover Problems

The DoD designated the period September 1, 1999, through March 31, 2000, as the "Y2K Date Transition Period." This period encompassed possible events occurring from the 9/9/99 date and February 29, 2000, leap year date. To prepare for the unprecedented nature of Y2K, DoD developed procedures to identify, report, and respond effectively to global Y2K events.

In January 1999, DoD formed a Year 2000 Consequence Management Integrated Process Team consisting of representatives from all elements of the Department. The team reviewed guidance, processes, and procedures for providing domestic Military Support to Civil Authorities (MSCA) and Foreign Disaster Assistance. The team also reviewed the organizational structure, processes, and procedures necessary to maintain operational readiness while responding to global requests for assistance. Based on recommendations made by the team, DoD:

- Acted to maintain the department's operational readiness and preeminence its national security responsibilities with consequence management requirements.
- Developed a decision support strategy to ensure DoD resources were applied in the most effective and efficient manner possible.
- Developed the Y2K Decision Support Activity (DSA) to monitor critical defense infrastructures, global public broadcasts, FEMA broadcasts, and the Internet. The DSA provided early warning, infrastructure performance, and resulting decision-support information to the Executive Secretariat, the DoD senior leadership, and the President's Council on Y2K Information Coordination Center.
- Developed specific Y2K training materials to ensure everyone involved in MSCA knew the specific methods for dealing with Y2K-related requests.
- Established an information flow to receive, track, and respond to requests for MSCA from FEMA and Foreign Disaster Assistance requests from Department of State.





Global Outreach

Russia

The U.S. and Russia worked on mutual Y2K-related national security concerns in five areas. The areas included Y2K Technology Management, Missile Warning, Nuclear Command

and Control, Nuclear Stockpile Security, and Special Communications Links. Each effort had a lead agency in charge with overall coordination conducted by the OSD Y2K Outreach Office.

Y2K Management

The OSD Y2K Outreach Office was lead agency responsible for the Y2K technology management effort. The purpose of the initiative was to exchange Y2K management program information, general status, and management experiences to provide mutual assistance in managing the problem, as well as understand each other's management plans and progress. Several meetings in Moscow permitted the two countries to exchange ideas on how best to manage the transition period. Russia decided to take an approach similar to the U.S. to meet its Y2K challenges.

Missile Warning

OSD Policy and the Joint Staff were lead agencies for the missile warning initiative. The purpose of the effort was to reduce the risk of misunderstandings from missile early warning systems. Other participants included OSD Staff (C3I), U.S. Space Command and North American Aerospace Defense Command, and the Air Force. The Center for Year 2000 Strategic Stability (CY2KSS) was established in Colorado Springs, CO, and operated over the transition period. The CY2KSS was manned by U.S. and Russian participants who jointly monitored missile early warning status and ensured there were no misunderstandings by either country.

Nuclear Command and Control

U.S. Strategic Command was lead for Nuclear Forces Command and Control initiative, which had two purposes. The first was to exchange nuclear specific Y2K management program information, general status, and management experience to assist each other in managing the problem, as well as understand each other's management plans and progress. The second was to discuss plans for managing Y2K when it arrived to prevent misunderstandings during the Y2K transition. Other participants included OSD Staff (Policy, C3I, Public Affairs, and functional experts), Joint Staff, U.S. Space Command and the North American Aerospace Defense Command, and Service Components. The participants worked with Russian Strategic Rocket Forces representatives to address mutual concerns and remedies.

Nuclear Stockpile Security

The Defense Threat Reduction Agency (DTRA) was lead agency for the nuclear stockpile security initiative. The purpose was to ensure control, security, and accountability of Russian nuclear materials, including stockpiles, weapons labs, and associated technology during the Y2K transition. Other participants included OSD Staff (Policy, C3I, and functional experts), Joint Staff, U.S. Strategic Command, and Service Components. The participants worked with Russian Ministry of Defense counterparts on specific action areas. Russia identified the location of 50 monitoring centers to meet security requirements and DTRA worked with the Russian Ministry of Defense to establish and equip the centers for Y2K transition period operations.

Special Communication Links

The Defense Information Systems Agency (DISA) was lead agency for the Special Communications Links initiative. The purpose was to ensure reliable communications between U.S. and Russian national political and military leaders during the Y2K transition. Other participants included OSD Staff (Policy, C3I, Public Affairs, and functional experts), Joint Staff, U.S. Strategic Command, and Service Components. Extensive work was conducted during the final months to assess existing communications links, upgrade various segments to ensure full Y2K compliance, and install additional redundancy and capability for the transition period.

Host Nation Support

The OSD Y2K Outreach program supplemented the extensive work of the Joint Staff, Service components, and defense organizations to address Y2K issues and ensure DoD could continue operations during the Y2K transition period. In many cases the emphasis for these prior efforts was placed on determining the installation's internal ability to manage Y2K challenges and did not necessarily address the capabilities of the host nations to provide continued support to overseas operating locations and missions.

The Y2K Outreach office expanded the overall DoD focus to "look beyond the fence" thus determining if and to what extent host nations could continue important support services during the Y2K transition period. The ultimate goal of the expanded efforts was to provide the CINCs and Service components the information they needed to determine vulnerabilities and conduct effective planning for continuity of operations and contingencies. Host nation sectors of primary concern included energy, telecommunications, water, wastewater, transportation, air traffic control services, medical services, and safety and security.

OSD Y2K Outreach worked closely with the Joint Staff, the Services, and CINC Y2K offices to determine which installations and support sectors required additional investigation to support planning efforts. The main geographic areas of interest for these efforts were Europe, South West Asia, and the Pacific/Asia. Specific locations were selected for assessment and teams were formed to visit the locations and meet with U.S. and host nation representatives. Each of the visits required extensive coordination with the State Department, embassies, CINC Y2K offices, DoD commands and components, and other U.S. Government (USG) organizations to schedule meetings and visits within the host nations. Each team was tailored to meet specific tasks and information requirements.

Information developed during the visits, continued research, coordination of information associated with other USG agency efforts, and additional details provided by operating locations in host countries provided a much better account of what to expect during the transition. In addition, the extensive level of coordination led to additional sources of information and increased the awareness of various issues among all participants. The combined contributions of all USG agencies provided a much better assessment of what DoD and other USG agencies could expect during the transition in overseas operating locations. Specific attention was paid to NATO, Supreme Headquarters Allied Powers Europe (SHAPE). OSD Y2K Outreach established working relationships with the SHAPE Y2K Program Management Office and provided appropriate technical expertise as SHAPE developed its Y2K management plans.

Risk Mitigation Policies

Consequence Management

The Department of Defense worked with other Federal agencies on consequence management and continuity of operations planning and recognized the potential for multiple competing demands for DoD resources throughout the Y2K date transition period. Because of this, in January 1999, the Department conducted a high level review of its "consequence management" policies, procedures, and organizations. Actions taken after the review ensured DoD was prepared to support a potentially increased number of requests for both domestic and international assistance.

First priority was to ensure DoD's ability to conduct ongoing or imminent support to the National Command Authorities, warfighting, peacekeeping, intelligence, nuclear command and control, or critical infrastructure protection operations. Consequently, approval by the Secretary of Defense, or his designated representative, was required before committing organizations and assets engaged in Priority 1 activities to support Y2K-related requests for assistance.

Likewise, the approval of the Chairman of the Joint Chiefs of Staff, or his designated representative, was required before committing assets or organizations engaged in Priority 2 activities to support Y2K-related requests for assistance.

Other units could provide support to civil authorities with first priority to maintenance of public health and safety and second priority to maintenance of the economy and the nation's quality of life.

Throughout 1999, DoD actively collaborated with federal agencies and organizations to further the Department's (and the Nation's) ability to develop and exercise the information flow and procedures necessary to respond effectively to Y2K-related events.

Configuration Management

The DoD issued a policy, "Limitation on Configuration Changes to Y2K-Compliant Systems," on August 20, 1999, to prevent jeopardizing system compliance by further modifications. This policy gave final decision-making authority to CINCs and ensured decisions on fielding or modifying systems included assessment of risks to current and future operations.

The importance of configuration management, including centralized visibility, was one of the important lessons of Y2K. In addition, preparation for Y2K also highlighted difficulty in maintaining positive control of configuration management activities.

Internet Connectivity

As part of its Y2K preparations, DoD issued a policy, "Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), on August 22, 1999, to ensure all DoD component systems connected to the internet met minimum security requirements. This policy required all connections to the Internet be through NIPRNet gateways managed by the Defense Information Systems Agency.

As DoD organizations worked to secure Internet connections, a collective appreciation for DoD's reliance on the Internet and on its vulnerabilities was gained. One of the challenges in achieving information assurance will be to mitigate DoD vulnerability to Internet weaknesses.

Community Conversations

During the summer months of 1999, parallel to and in support of the President's Council on Year 2000 Conversion, DoD launched a program of Community Conversations to promote awareness of local issues and encourage proactive contingency planning. The DoD implemented this concept across all Military Departments with a continuing effort through the end of 1999 to raise community awareness for day one planning and personal preparedness.

Major installations hosted many events engaging civic leaders and the general populace in open dialogue. The materials and centralized guidance provided by the OSD staff promulgated a common and consistent message to coincide with that of the President's Council. Materials for Community Conversations and other Y2K Business Continuity and Contingency Planning items of interest were made available at the DoD Y2K Contingency Planning web site. Over 200 DoD installations engaged in "Community Conversations" with their surrounding civilian communities to share information regarding Y2K efforts.

Code Screening

The Department purchased tools to aid in Y2K renovation and testing that proved to be not only cost effective, but also a critical part of the DoD risk mitigation effort. These tools were industrial-strength quality assurance and test support software useful in Y2K compliance testing, code analysis, regression testing, and code quality assessment. As a risk reduction measure, the military departments, intelligence community, and defense agencies screened large amounts of computer code with multiple tools.

Code screening turned out to be a very effective final screening effort when coupled with an effective configuration management process. This effort had many positive benefits for future information assurance and information technology management initiatives.

External Auditing

External auditing was a major factor in DoD's Y2K success and Y2K was the most audited non-financial event in federal government history. Every aspect of the DoD Y2K program involved external auditing. For systems Y2K compliance, the DoD Y2K Management Plan provided guidance on independent verification and validation of system Y2K compliance. A mix of independent contractors, Inspectors General, other internal audit agencies, and the Government Accounting Office conducted independent verification and validation efforts. Large scale integration testing was audited by military department inspectors general, the DoD Inspector General, and the General Accounting Office. Finally, several risk mitigation efforts involved external auditing, such as configuration management and code screening.

The DoDIG and Military Inspectors General

The Office of the Assistant Inspector General for Auditing, DoD, in accordance with an informal partnership with the DoD Chief Information Officer, provided substantial support to effective oversight of the DoD Y2K program. Since its initial Y2K audit efforts in 1997, the DoD Inspector General conducted 181 Y2K audits, devoting over 180 staff years, or more than 30 percent of its audit staff, to Y2K audits during FY 1999. Staff costs for Y2K audits during Fiscal Years 1998 and 1999 exceeded $16 million.

The Military Department Inspectors General provided independent assessments of DoD Y2K compliance management and implementation by making Y2K a special inspection item.

The General Accounting Office (GAO)

GAO auditors played a similar function in advising the senior leadership. The DoD followed GAO's guides and templates for each phase of remediation as well as GAO guides for contingency planning and Day One planning.

Summary of DoD Y2K program

The complex and wide-ranging DoD Y2K program resulted in an extraordinary level of success for the century rollover. In addition, there were many benefits gained that will pay dividends in future information technology management and information assurance efforts.

DoD Y2K Lessons Learned

There were many lessons learned from the Y2K experience at every echelon of DoD. The most important of these have been distilled and grouped in three categories: Enterprise-Wide lessons applying to DoD and other federal agencies, Chief Information Officer lessons that apply to DoD efforts to achieve compliance with the provisions of the Clinger-Cohen Act of 1996, and Warfighting lessons learned from the Joint Staff and CINCs.

Enterprise-Wide Lessons Learned

Hard work paid off - everything worked

Across DoD, thousands of systems continued to function across the century rollover. In cases where there were problems, contingency plans worked and assets were available to quickly respond to problems. This success is a testament to the rigor of system compliance efforts, contingency and continuity of operations planning, and superb execution throughout the DoD.

Government worked

The success achieved on Y2K is a testament to hard work by government employees and contractors across the federal government. Interagency efforts coordinated by the President's Council on Y2K, including the federal sectors and high impact programs, produced the Y2K success. The cooperation between government and industry worked, as did an unprecedented level of cooperation between governments. Despite a high level of ongoing military operations, the job got done right.

Warfighting/Readiness Issue

In the summer of 1998, senior leaders recognized that Y2K was a Chief Executive Officer problem - not just a Chief Information Officer problem. To energize DoD, the Secretary of Defense directed the DoD leadership to treat Y2K as a readiness issue in August of 1998. This turning point ensured all members of DoD understood the necessity of cooperation to achieve success in preparing for Y2K and galvanized preparedness efforts.

Horizontal Problems versus Vertical Organizations

The DoD and government are organized along vertical lines, however, many problems of the 21st century are horizontal in nature, such as encryption andY2K. Management for success requires a team oriented approach and close Chief Executive Officer focus to ensure successful resolution of key organizational problems where responsibility does not lie solely with one major organizational component. The Y2K problem showed the utility of standardized guidance and performance measurement tools to focus efforts across the organization coupled with proactive external auditing and effective management response.

Increased Dependence on Information Technology Systems

Business process improvements have increased dependence on information technology systems -- a potential vulnerability. One example is “Just in time” logistics. The DoD achieved success by teamwork with our business partners. The DoD required confidence in its vendor partners, which resulted from close teamwork and other measures, such as surveying thousands of U.S. companies to check Y2K readiness.

Importance of Computer Professionals

In preparing for Y2K, one important outcome was that warriors realized they needed the computer professional. DoD culture emphasizes warfighters; not computer professionals. After the Y2K effort, all now recognize that DoD needs to adapt to recognize the significance and contributions of information technology professionals.

Chief Information Officer Lessons Learned

Importance of Effective Chief Information Officers

DoD CIO’s must have a close working relationship with warfighters and senior leaders to make best use of Information Technology. Since a high level of information technology supports every part of the DoD, effective participation by the Chief Information Officer in business decisions was clearly recognized by all. These efforts span the DoD business processes of warfighting, support operations, and organizing, training, and equipping.

Collaborative Partnerships

The efforts of DoD in working with industry and allies had a large payoff in many ways, not just for Y2K. The increased appreciation for the level of interdependence and linkages of IT systems had major benefits for daily operations and planning.

One previous program, the Enterprise Software Initiative, proved extremely successful in making industrial-strength quality assurance and test support software useful in Y2K compliance testing, code analysis, regression testing, and code quality assessment widely available throughout DoD. Other collaborative partnerships involving prime vendors and electronic business have great potential for further benefits.

Centralized Guidance/Decentralized Execution

The use of one capstone document, the DoD Y2K Management Plan, to provide centralized policies, procedures, and performance measurement tools was a key element of DoD's success in Y2K. The scope, magnitude, and complexity of the Y2K problem for DoD made decentralized execution a necessity. Making centralized guidance widely available on-line, fostered teamwork and helped ensure all organizational elements focused on the same goals.

Accurate Inventory of Information Technology

Centralized visibility of assets is fundamental to information technology management (e.g., acquisition, configuration management, and information assurance). Timely and accurate performance measurement is essential to quality management oversight. The DoD Y2K database was used to ensure visibility and standardized reporting of progress.

By making the database available on-line to all DoD components, including the Intelligence Community, the reporting process was compressed. This allowed the DoD Y2K database to be used as an accurate and comprehensive measure of DoD progress in many areas of Y2K. The DoD Y2K database will be used as the basis for compliance with the provisions of Public Law 106-79, DoD Appropriations Act for Fiscal Year 2000, concerning registration and certification of information technology systems by the Chief Information Officer.

Teamwork with External Oversight and Audit Organizations

One of the major success factors for DoD on Y2K was the transparency resulting from including Congress, GAO, Office of Management and Budget, and the DoD Inspector General in all aspects of the DoD Y2K effort. Representatives attended monthly Y2K Steering Committee meetings chaired by the Deputy Secretary of Defense and remained fully apprised of DoD status on all aspects of Y2K.

Warfighting Lessons Learned

The Joint Staff hosted a conference for CINC, OSD, and Defense Agency representatives on February 1-2, 2000, to address Y2K lessons learned.

Overview

Dealing with Y2K required parallel execution of many parts of a complex process. Success was enabled by leadership; unprecedented close relationships between DoD, the Joint Staff, and the CINCs, Services, and Defense Agencies and Activities; and a willingness and ability to re-focus workforces as the collective understanding of the Y2K problem changed.

Success on Y2K had many side-benefits, including improved knowledge of systems, system architectures, and interdependencies; mission versus purely system focus; continuity of operations plans and contingency plans that worked.

Joint Staff and CINC Lessons Learned

Joint Staff and CINC specific lessons learned included rollover organizations, use of reserve forces, and the role of Joint Staff and CINC Chief Information Officers.

Rollover Organizations

One of the lessons learned from Y2K rollover preparations and operations was that well staffed organizations paid off. A clear focus on Y2K failures, millennium groups and terrorist attacks, and computer network attacks was maintained and served well. During rollover reporting, however, it became clear that current report formats work well for operational issues but are not well structured for capturing the impacts of information technology problems on warfighting operations. The Joint Staff and CINC staffs are actively working to restructure the report within the next six months.

Use of Reserve Forces

Reserves and contractor support were essential to the Y2K effort. Many individuals were called to active duty to support various aspects of the Y2K effort. In some cases, the lead times and processes to obtain reserve forces varied among the reserve components. Once called up, however, these individuals provided essential support to enable successful execution of Y2K efforts in the combatant commands and their components.

Joint Staff and CINC Chief Information Officers

Based on work during Y2K, it became clear that Chief Information Officer roles, responsibilities, and implementations were inconsistent across the combatant commands and the Joint Staff. The importance of Chief Information Officers was clearly recognized and DoD is developing a plan of action to establish them on the Joint Staff and CINC staffs.

DoD-Wide Recommendations

The DoD-wide lessons learned identified during the Joint Staff Y2K conference include data reuse, management processes, configuration management, and testing.

Data Reuse

Many types of information and data were centrally collected for Y2K, including OSD, Joint Staff, CINC, Military Department, and Defense Agency databases of Y2K-related information on specific systems across the information technology spectrum. The Y2K "thin-lines" and mission architectures provided a view of the critical processes and interrelationships of selected critical warfighting missions and tasks. Contingency plans and continuity of operations plans were developed, which proved to be a valuable training tool.

This data has many potential reuses, including information assurance; critical infrastructure protection; joint operational architectures; and refinement of deliberate and contingency planning. The data is also potentially useful for incorporating information assurance, critical infrastructure protection, interoperability, and configuration management into military exercises; and for enhancing DoD information technology management.

As an example, DoD will convert the DoD Y2K database for use in registering and certifying DoD information technology systems under section 8121 of the Department of Defense Appropriations Act for Fiscal Year 2000.

Management Processes

The integration of Chief Information Officers and Warfighters was key to Y2K success. For example, the construction of thin line architectures provided invaluable insights into warfighting tasks and the reliance on information technology systems. Coupled with the operational evaluations that tested system interoperability, a collective appreciation was realized for the necessity to carefully manage information technology systems supporting warfighting operations. Based on this lesson learned, the Joint Staff and CINCs will develop joint operational architectures for all warfighting mission areas.

Configuration Management

The CINCs require insight into their system configurations to allow analysis of the benefits and risks of fielding information technology systems or configuration changes. To provide this insight, the DoD Y2K configuration management limitation policy will be allowed to expire on March 15, 2000. The Joint Staff and CINCs will work to develop a proposed framework for sustaining CINC insight into system configurations.

Another factor in DoD's success on Y2K was the use of software tools to support configuration management and technical problem isolation. The tools continue to be used on a daily basis and are required for future operations. Consequently, DoD will renew licenses for independent verification and validation tools for further use in configuration management.

Another lesson learned by warfighting functional proponents was information technology management programs are not well defined, adequately resourced, nor are program requirements fully defined. The CINCs and Joint Staff will continue working to ensure information technology managers fully define program requirements and that resources are provided once requirements are defined.

Testing

The warfighting context provided by CINC operational evaluations was critical to DoD Y2K success. The operational evaluations validated information technology testing and evaluation, including examination of contingency plans. In the future, the department will incorporate information assurance, critical infrastructure protection, interoperability, and configuration management issues into routine CJCS, CINC, and Military Department exercise and training programs.

Another benefit of the Y2K effort was the appreciation of how battle labs added an invaluable dimension to CINC operational evaluations. These centralized testing facilities contained the necessary resources and expertise to enable successful information technology testing of operational architectures.

Summary of Actions

Based on lessons learned from the Y2K effort, the Joint Staff will take the following actions in coordination with the CINCs and other DoD components:

- Review suitability of Operational Reports for global information technology reporting
- Streamline and standardize Reserve call-up procedures
- Develop a resource strategy for large-scale CINC information technology operations
- Develop a plan to establish Chief Information Officers on the Joint and CINC staffs
- Institutionalize integration of Chief Information Officers and Warfighters
- Consider databases, thin lines, and leftover documentation for reuse in information assurance, critical infrastructure protection, joint operational architectures, standing contingency plans, exercises, and information technology management
- Develop prototype Joint Operational Architectures
- Propose framework for sustaining CINC insight into system configurations
- Renew licenses for existing independent verification and validation tools
- Define information technology program requirements and resource accordingly
- Incorporate information assurance, critical infrastructure protection, interoperability and configuration management into routine exercises and training

Effective Implementation of Lessons Learned – The Bottom Line

Four aspects of the Y2K process are vital to implementing Y2K lessons learned:

- Senior leadership must remain engaged in information technology management
- Every level of management and operations must understand the warfighting processes supported by information technology systems
- Information technology management requirements must be defined and understood at all levels

- Information technology management functions must receive enough resources to meet the requirements

The combination of these three groups of DoD lessons learned from Y2K (Enterprise-Wide, Chief Information Officer, and Warfighting), provide a roadmap for improving information technology management. The DoD Chief Information Officer will use the DoD Chief Information Officer Executive Board to monitor implementation of Y2K lessons learned on the OSD staff, Joint Staff, Military Departments, and Defense Agencies. Implementing and institutionalizing these lessons learned will better position DoD to address similar “horizontal” problems, such as information assurance.

Conclusion

The DoD efforts to address the Y2K problem resulted in major improvements to information technology management throughout the department. Increased appreciation at all levels for DoD’s reliance on information technology and the role of the Chief Information Officer, the shift in focus from systems to core missions and functions, greatly improved contingency and continuity of operations plans, and improved risk mitigation measures are all positive outcomes of the Y2K experience.

The lessons learned from Y2K provide a clear roadmap for improving information technology management within DoD and for expediting compliance with all provisions of the Clinger-Cohen Act of 1996. The DoD Y2K effort has laid a firm foundation for longer term improvements in managing and protecting information technology systems and critical infrastructure.